UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The person of Antonio RAGSDALE (DOB: XX/XX/1989); and 2744 N. 9th St, Milwaukee, Wisconsin, and any outbuildings, garages, or tenant designated storages, lockers, or other areas associated with this address in addition to a black Chevrolet Avalanche bearing Iowa license plate number LMK514	)	Case No. 25-807M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 2/18/2025 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for ____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 2/4/2025 @ 10:28 a.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be searched

1. The person of Antonio RAGSDALE (DOB: XX/XX/1989); and

2. The property to be searched is: 2744 N. 9th St., Milwaukee, Wisconsin 53206, further described as a light cream, two-story townhome residence, with white trim and a brown roof. The structure is near the corner of N. 9th St. and W. Hadley St. in the City and County of Milwaukee, Wisconsin. The white entrance door is located on 9th St, with the numbers "2744" affixed above the mailbox next to the entrance door. This address is referred to as the "PREMISES." This search also includes any outbuildings, garages, or tenant designated storages, lockers, or other areas associated with this address in addition to a vehicle; specifically, a Black Avalanche bearing Iowa license plate number LMK514 associated with RAGSDALE.

Photos of front and side view of 2744 N. 9th St, Milwaukee, Wisconsin.

Photos of front and side view of 2744 N. 9th St, Milwaukee, Wisconsin.

ATTACHMENT B

Items to be seized

1. Controlled Substances;

2. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;

3. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;

4. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;

5. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;

6. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

7. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

8. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

9. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

10. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

11. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

12. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

13. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and

14. Computers, cellular telephones, or storage media used as a means to commit the violations described above;

15. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of ANTONIO RAGSDALE to the fingerprint scanner of a device found at the premises; and/or (2) hold a device found at the premises in front of ANTONIO RAGSDALE's face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The person of Antonio RAGSDALE (DOB: XX/XX/1989); and 2744 N. 9th St, Milwaukee, Wisconsin, and any outbuildings, garages, or tenant designated storages, lockers, or other areas associated with this address in addition to a black Chevrolet Avalanche bearing Iowa license plate number LMK514	Case No. 25-807M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

see Attachment A,

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841;	Possession with intent to distribute controlled substances and distribution of controlled substances;
18 U.S.C. § 924(c)	Use of a firearm in furtherance of drug trafficking

The application is based on these facts:

see attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

GARY M ROY

Digitally signed by GARY M ROY
Date: 2025.02.04 09:58:12 -06'00'

Applicant's signature

Gary Roy, HSI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 2/4/2025

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Gary Roy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, a residential dwelling, a vehicle and a person, and the extraction of evidence from those locations and that person described in Attachment B.

2. I am a Special Agent with the federal Homeland Security Investigations ("HSI"), and have been so employed since 2018. Before that time, I was a Patrol Agent with the United States Border Patrol since 2007. In my capacity as an HSI special agent, I have investigated various federal crimes, including violations of Title 18, United States Code, Section 922, and Title 21, United States Code, Sections 5861(d) and 5861(f).

3. During my career in law enforcement, I have investigated violations of federal narcotics laws and related violations, including federal firearms offenses. Based on my training, experience, and participation in firearms and drug trafficking investigations, I am familiar with the appearance and street names of various drugs, including marijuana, methamphetamine, heroin, cocaine, cocaine base (crack cocaine), and ecstasy. I am also familiar with the appearance and street names for firearms and firearm accessories, including machine-gun conversion devices, also known as "switches." I know that firearm traffickers often use various communication devices to conduct trafficking operations, and that traffickers often communicate on cell phones using text messages and direct connect cell phone capabilities. I know that firearms traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion and control: firearms; ammunition; and records or receipts pertaining to such.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. Based upon the evidence gathered to date, I submit that there is probable cause to believe that Antonio RAGSDALE (DOB 06/10/1986) has committed the following violations: Title 21, United States Code, Sections 841(a)(1), Distribution of, and Possession with Intent to Distribute Controlled Substances; and Title 18, United States Code, Section 924(c), Possession of Firearms in Furtherance of Drug Trafficking; and, Title 18, U.S.C. Section 2. I further submit that there is probable cause that evidence of these criminal violations will be found at the location to be searched, as further described below and in Attachment A.

LOCATIONS AND PERSON TO BE SEARCHED

6. This warrant seeks authority to search the following location and person, more fully described in Attachment A, and to seize the evidence described in Attachment B:

a. 2744 N. 9th St., Milwaukee, Wisconsin 53206, further described as a light cream, two-story townhome residence, with white trim and a brown roof. The structure is near the corner of N. 9th Street and W. Hadley Street in the City and County of Milwaukee, Wisconsin. The white entrance door is located on 9th Street, with the numbers "2744" affixed above the mailbox next to the entrance door. This address is referred to as the "PREMISES."

b. The person of Antonio RAGSDALE (DOB 06/10/1986).

PROBABLE CAUSE

7. On February 4, 2025, the United States Marshals Service (USMS) Eastern Wisconsin Violent Offender Task Force (EWVOTF), of which Special Agent (SA) Gary Roy is a member of, executed an arrest warrant for Antonio RAGSDALE (RAGSDALE) at his residence of 2744 N. 9th Street, Milwaukee, Wisconsin 53206 (the PREMISES).

8. RAGSDALE is wanted out of Black Hawk County, Iowa for violations to include controlled substance violations, failure to affix drug tax stamps, and a failure to appear for a willful injury. RAGSDALE is also a previously convicted felon.

9. During the execution of the arrest warrant, EWVOTF members knocked and announced their presence at the door to the PREMISES. In response, a male voice asked who was at the door. EWVOTF members repeated their announcements, identifying themselves as the U.S. Marshals and called out for RAGSDALE to come to the door and surrender peacefully. During the communication with the male voice, an EWVOTF member looking through the front window observed RAGSDALE in the living room. Previously, EWVOTF members had reviewed a photograph of RAGSDALE and the person inside the living room matched the photograph. As EWVOTF members gave RAGSDALE commands to open the door, task force members observed RAGSDALE retreating towards the back of the house. Subsequently, EWVOTF members at the door, who are familiar with the sound of a gun racking, heard what sounded like the distinct racking of a firearm. In the driveway, task force members also observed a vehicle known to be associated with RAGSDALE; that is, a Black Avalanche, bearing license plate LMK514 issued out of Blackhawk, Iowa where the arrest warrant was issued

10. Based upon RAGSDALE's failure to comply with orders to open the door, and hearing the sound of the charging of a firearm, EWVOTF members breached the door and gained

entry to the front living room. Upon opening the door, EWVOTF members observed RAGSDALE standing outside a bedroom door. EWVOTF members gave RAGSDALE commands to place his hands in the air and walk towards them. RAGSDALE responded by lying on the ground and crawling his way towards EWVOTF members near the front door. RAGSDALE was taken into custody without further incident.

11. At the time RAGSDALE was taken into custody, he was clothed only in boxer underwear. RAGSDALE complained about the cold and asked if EWVOTF members could obtain clothes for him. EWVOTF members asked RAGSDALE where his clothes were located and RAGSDALE indicated the bedroom near where he had been previously standing. EWVOTF members then entered the PREMISES and began clearing procedure of the PREMISES in order to make it safe and secure.

12. As EWVOTF members were clearing the PREMISES, they observed a clear, crystal-like substance wrapped in a clear plastic bag, in a container with a digital drug scale, in plain view located near the couch in the living room. The properties of the crystal-like substance appeared to be similar to the properties of crystal methamphetamine. As EWVOTF members cleared the bedroom which RAGSDALE indicated was his, EWVOTF members observed an active CPAP machine on the nightstand. The drawer of the nightstand was open, and in the drawer a black handgun in a cloth holster was observed, also in plain view. Based upon my training and experience, I am aware, based upon a visual inspection of the suspected crystal methamphetamine, which was located along with a digital scale commonly used for narcotics distribution, that RAGSDALE possessed the suspected methamphetamine for distribution. Additionally, given the proximity of the firearm to the narcotics (i.e., approximately four feet), I further believe that RAGSDALE possessed the firearm in furtherance of drug trafficking.

13. Upon observing what appears to be controlled substances, indicia of narcotic distribution, and a firearm in plain view, EWVOTF members froze the PREMISES pursuant to an application of a search warrant.

14. After RAGSDALE was taken into custody, the PREMISES homeowner, later identified as Larae Ragsdale arrived on scene. Your affiant interviewed Ragsdale, who stated she was the homeowner and was aware RAGSDALE had active warrants. I asked Larae if the CPAP machine inside the bedroom belonged to her, to which she stated it belonged to RAGSDALE. I asked Larae if she owned any firearms inside the house, to which Larae stated she did not and was currently seeking to get a license. I asked Larae if she knew of any narcotics to be in the house, to which Larae stated she only smokes weed. This interview was recorded on body camera.

15. Based on the investigation thus far, I submit there is probable cause to believe that evidence associated with the criminal violations detailed above will be located within the PREMISES and on the person of Antonio RAGSDALE.

16. Further, affiant is aware, based on training, experience, and information provided from other members of law enforcement, that evidence of illegal firearm possession is commonly found on electronic devices such as computers and cellular phones. Affiant is aware that those engaged in the importation, sale, or possession of firearms often take, or cause to be taken, photographs, video, and other visual depictions of firearms, and typically keep and maintain these photographs, video, and other visual depictions in cellular phones located on their person or on other mediums such as computers and hard drives in areas where they have exercised dominion and control.

17. Affiant is aware that it is common for those who possess and traffic firearms, to purchase and maintain ownership of firearms for long periods of time. Firearms are a commodity

that are often held for long periods of time.

18. Affiant is aware that cellular phones can be used to store information including text messages, multimedia messages, and a history of incoming and outgoing calls, contact/address book information, photographs, videos, GPS and other location information, internet search history, and other data.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

8. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

9. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

i. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

ii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

iii. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

iv. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

10. *Forensic evidence.* As further described in Attachment B, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have

geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

v. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

11. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often

requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

iii. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

CONCLUSION

13. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and person of Antonio RAGSDALE (DOB XX/XX/1986), described in Attachment A, and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

1. The person of Antonio RAGSDALE (DOB: XX/XX/1989); and

2. The property to be searched is: 2744 N. 9th St., Milwaukee, Wisconsin 53206, further described as a light cream, two-story townhome residence, with white trim and a brown roof. The structure is near the corner of N. 9th St. and W. Hadley St. in the City and County of Milwaukee, Wisconsin. The white entrance door is located on 9th St, with the numbers "2744" affixed above the mailbox next to the entrance door. This address is referred to as the "PREMISES." This search also includes any outbuildings, garages, or tenant designated storages, lockers, or other areas associated with this address in addition to a vehicle; specifically, a Black Avalanche bearing Iowa license plate number LMK514 associated with RAGSDALE.

Photos of front and side view of 2744 N. 9th St, Milwaukee, Wisconsin.

Photos of front and side view of 2744 N. 9th St, Milwaukee, Wisconsin.

ATTACHMENT B

Items to be seized

1. Controlled Substances;

2. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;

3. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;

4. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;

5. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;

6. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

7. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

8. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

9. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

10. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

11. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

12. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

13. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and

14. Computers, cellular telephones, or storage media used as a means to commit the violations described above;

15. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of ANTONIO RAGSDALE to the fingerprint scanner of a device found at the premises; and/or (2) hold a device found at the premises in front of ANTONIO RAGSDALE's face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.